AO 93C (08/18) Warrant by Telephone or Other Reliable Electronic Means ❒ Original ❒ Duplicate Original

UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* (1) The Biller Hotel property located at 725 N 22nd St, Milwaukee, WI 53233, limited to Room 105. The Biller Hotel is a four story, brick facade building with a green awning over the front entrance. The hotel is divided into multiple different individual rooms. The search will be limited to the room labeled 105. (2) the person of James Bernier, DOB 10/4/1986	)	Case No.23-855M(NJ)

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the Eastern District of Wisconsin *(identify the person or describe the property to be searched and give its location)*:

See Attachment A

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment B

YOU ARE COMMANDED to execute this warrant on or before 2/9/2023 *(not to exceed 14 days)*

xx❒ in the daytime 6:00 a.m. to 10:00 p.m. ❒ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Honorable Nancy Joseph .

(United States Magistrate Judge)

❒ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

❒ for _____ days *(not to exceed 30)* ❒ until, the facts justifying, the later specific date of _____ .

Date and time issued: 1/26/2023 @ 11:19 a.m.

Nancy Joseph

Judge's signature

City and state: Milwaukee, WI

Honorable Nancy Joseph, U.S. Magistrate Judge

Printed name and title

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name(s) of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A
DESCRIPTION OF LOCATIONS TO BE SEARCHED

(1) The Biller Hotel property located at 725 N 22nd St, Milwaukee, WI 53233 (photo below) limited to Room 105. The Biller Hotel is a four story, brick façade building with a green awning over the front entrance. The hotel is divided into multiple different individual rooms. The search will be limited to the room labeled 105.

(2) the person of James Bernier, DOB 10/4/1986.

ATTACHMENT B

LIST OF ITEMS TO BE SEIZED

1. Cell phones, computer(s), computer hardware, computer software, computer related documentation, computer passwords and data security devices, videotapes, video recording devices, video recording players, and video display monitors that may be, or are used to: visually depict child pornography or child erotica; display or access information pertaining to a sexual interest in child pornography; display or access information pertaining to sexual activity with children; or distribute, possess, or receive child pornography, child erotica, or information pertaining to an interest in child pornography or child erotica.
2. Any and all computer software, including programs to run operating systems, applications (such as word processing, graphics, or spreadsheet programs), utilities, compilers, interpreters, and communications programs.
3. Any and all notes, documents, records, or correspondence, in any format and medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and handwritten notes) pertaining to the possession, receipt, or distribution of child pornography as defined in 18 U.S.C. § 2256(8) or to the possession, receipt, or distribution of visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2).
4. In any format and medium, all originals, computer files, copies, and negatives of child pornography as defined in 18 U.S.C. § 2256(8), visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2), or child erotica.

5. Any and all diaries, address books, names, and lists of names and addresses of individuals who may have been contacted by the operator of any device by use of the computer or by other means for the purpose of distributing or receiving child pornography as defined in 18 U.S.C. § 2256(8) or visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2).
6. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and handwritten notes), identifying persons transmitting, through interstate or foreign commerce by any means, including, but not limited to, by the United States Mail or by computer, any child pornography as defined in 18 U.S.C. § 2256(8) or any visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).
7. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, other digital data files and web cache information) concerning the receipt, transmission, or possession of child pornography as defined in 18 U.S.C. § 2256(8) or visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).
8. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) concerning communications between individuals about child pornography or the existence of sites on the Internet

that contain child pornography or that cater to those with an interest in child pornography.

9. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) concerning membership in online groups, clubs, or services that provide or make accessible child pornography to members.

10. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) that concern any accounts with an Internet Service Provider.

11. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) that concern online storage or other remote computer storage, including, but not limited to, software used to access such online storage or remote computer storage, user logs or archived data that show connection to such online storage or remote computer storage, and user logins and passwords for such online storage or remote computer storage.

12. Any and all cameras, film, videotapes or other photographic equipment.

13. Any and all visual depictions of minors.

14. Any and all address books, mailing lists, supplier lists, mailing address labels, and any and all documents and records, in any format or medium (including, but not

limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files), pertaining to the preparation, purchase, and acquisition of names or lists of names to be used in connection with the purchase, sale, trade, or transmission, through interstate or foreign commerce by any means, including by the United States Mail or by computer, any child pornography as defined in 18 U.S.C. § 2256(8) or any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

15. Any and all diaries, notebooks, notes, and any other records reflecting personal contact and any other activities with minors visually depicted while engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

16. For any electronic storage device, computer hard drive, electronic device, or other physical object upon which electronic information can be recorded (hereinafter, "electronic storage device") that is called for by this warrant, or that might contain things otherwise called for by this warrant:

    a. evidence of who used, owned, or controlled the electronic storage device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

    b. evidence of software that would allow others to control the electronic storage device, such as viruses, Trojan horses, and other forms of malicious software, as

well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence indicating how and when the electronic storage device was accessed or used to determine the chronological context of electronic storage device access, use, and events relating to crime under investigation;

e. evidence indicating the electronic storage device user's location and state of mind as it relates to the crime under investigation;

f. evidence of the attachment to the electronic storage device of other storage devices or similar containers for electronic evidence;

g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the electronic storage device;

h. evidence of the times the electronic storage device was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the electronic storage device;

j. documentation and manuals that may be necessary to access the electronic storage device or to conduct a forensic examination of the electronic storage device;

k. contextual information necessary to understand the evidence described in this attachment.

17. Records and things evidencing the use of the Internet Protocol addresses to communicate with the internet, including:

a. routers, modems, and network equipment used to connect electronic storage devices to the Internet;

b. records of Internet Protocol addresses used;

c. records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

As used above, the terms "records" and "information" include all the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of electronic storage device or electronic storage; any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form.

During the execution of the search of the premises described in Attachment A, law enforcement personnel are authorized to press the fingers (including thumbs) of individuals found at the premises to the Touch ID sensor of device(s) or scan for facial recognition, such as an iPhone. Android, or Tablet, found at the premises for the purpose of attempting to unlock the device via fingerprint or facial recognition in order to search the contents as authorized by this warrant. If facial recognition is required, the subject(s) will remain still and look, with eyes open, at the camera for any devices seized in connection if this warrant for the purpose of attempting to unlock the device(s) in order to search the contents as authorized by this warrant.

UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

(1) The Biller Hotel property located at 725 N 22nd St, Milwaukee, WI 53233, limited to Room 105. The Biller Hotel is a four story, brick facade building with a green awning over the front entrance. The hotel is divided into multiple different individual rooms. The search will be limited to the room labeled 105. (2) the person of James Bernier, DOB 10/4/1986

Case No.23-855M(NJ)

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A

located in the Eastern District of Wisconsin, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☑ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. 2251(a)	Attempted production of child pornography
18 U.S.C. 2252(a)(2)	Receipt/distribution of child pornography
18 U.S.C. 2252(a)(4)(B)	Possession of child pornography

The application is based on these facts:

See attached affidavit

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Sarah Dettmering, FBI, Special Agent

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone *(specify reliable electronic means)*.

Date: 1/26/2023

Judge's signature

City and state: Milwaukee, WI

Honorable Nancy Joseph, U.S. Magistrate Judge

Printed name and title

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Sarah Dettmering, being first duly sworn, depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I have been employed as a Special Agent of the FBI, since January 2018, and am currently assigned to the Milwaukee Division as a member of the Milwaukee Child Exploitation and Human Trafficking Task Force. While employed by the FBI, I have investigated federal criminal violations related to child exploitation, and child pornography. I have received training to investigate child pornography and child exploitation crimes and have had the opportunity to observe and review examples of child pornography (as defined in 18 U.S.C. § 2256) in different forms of media including computer media. As a result of my training, experience, and discussions with other law enforcement officers assigned to investigate child pornography and child exploitation, I am familiar with methods by which electronic devices are used as the means for receiving, transmitting, possessing, and distributing images and videos depicting minors engaged in sexually explicit conduct. I have also received training and gained experience in interview and interrogation techniques with enhanced training specific to cybercrimes, social media search warrants, residential search warrants, interviews and interrogations of subjects of criminal investigations, as well as electronic device identification and forensic review.

2. The facts contained in this affidavit are known to me through my personal knowledge, training, and experience, and through information provided to me by other

law enforcement officers, who have provided information to me during the course of their official duties and whom I consider truthful and reliable.

3. Based upon the information described below, I submit that probable cause exists to believe that the subject, James Bernier (BERNIER), residing at the Biller Hotel, address: 725 N 22nd St, Room 105, Milwaukee, WI 53233 (SUBJECT PREMISES), utilizing the Discord account "Fu#9282" (SUBJECT ACCOUNT) has committed the crimes of attempted production of child pornography, in violation of Title 18, United States Code, Section 2251(a), receipt/distribution of child pornography in violation of Title 18, United States Code, Section 2252(a)(2), and possession of child pornography in violation of Title 18, United States Code, Section 2252(a)(4)(B). I further submit that evidence relating to this crime, more particularly described in Attachment B, can be found in the SUBJECT PREMISES, more particularly described in Attachment A.

4. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

DEFINITIONS

5. The following definitions apply to the Affidavit and Attachment B to this Affidavit:

a. "Child Pornography" is defined in 18 U.S.C. § 2256(8) as any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction

is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

b. "Chat," as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

c. The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

d. An "Internet Protocol address" (IP address) is a unique numeric address used by internet-enabled electronic storage devices to access the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every electronic storage device attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that electronic storage device may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static that is, long-term

IP addresses, while other computers have dynamic that is, frequently changed IP addresses.

e. "Minor" means any person under the age of eighteen years. See 18 U.S.C. § 2256(1).

f. The terms "records," "documents," and "materials" include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including writings and drawings), photographic form (including prints, negatives, videotapes, motion pictures, and photocopies), mechanical form (including printing and typing) or electrical, electronic or magnetic form (including tape recordings, compact discs, electronic or magnetic storage devices such as hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, smart cards, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

g. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person. See 18 U.S.C. § 2256(2).

h. "Visual depictions" include undeveloped film and videotape, and data stored on a computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).

i. "Website" consists of text pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from the web servers to various web clients via Hyper-Text Transport Protocol.

ELECTRONIC STORAGE DEVICES AND FORENSIC ANALYSIS

6. I am aware through training, experience, and consulting with other law enforcement agents/analysts with specialized knowledge and training in computers, networks, and Internet communications that to properly retrieve and analyze electronically stored (computer) data, and to ensure accuracy and completeness of such data and to prevent loss of the data either from accidental or programmed destruction, it is necessary to conduct a forensic examination of the electronic storage devices. To ensure such accuracy and completeness, it may also be necessary to analyze not only the electronic storage devices, but also peripheral devices which may be interdependent, the software to operate them, and related instruction manuals containing directions concerning operation of the device computer and software. As described above and in Attachment B, this application seeks permission to search and seize records that might be found on the proposed search location, in whatever form they are found. One form in which the records might be found is stored on a computer's hard drive, other storage media, within a hand-held electronic device such as a cellular telephone or a tablet device (e.g., an iPad device). Some of this electronic information, as explained below, might take a form that becomes meaningful only upon forensic analysis.

7. Based on my knowledge, training, and experience, I know that computer and other electronic device hardware, peripheral devices, software, documentation, and passwords may be important to a criminal investigation in three distinct and important respects.

a. The objects themselves may be instrumentalities used to commit the crime;

b. the objects may have been used to collect and store information about crimes (in the form of electronic data); and

c. the objects may be contraband or fruits of the crime.

8. I submit that if a computer or other electronic storage device is found on the premises, there is probable cause to believe those records will be stored in that electronic storage device, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that electronic storage device files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person deletes a file on an electronic storage device, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data. It follows that deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space

on the storage medium that is not currently being used by an active file for long periods of time before they are overwritten. In addition, if the electronic storage device uses an operating system (in the case, for example, of a computer, cellular telephone, or tablet device) the device may also contain a record of deleted data in a swap or recovery file.

b. Wholly apart from user-generated files, electronic storage device storage media in particular, computers' internal hard drives, contain electronic evidence of how the device was used, what it has been used for, and who has used it. This evidence can take the form of operating system configurations, artifacts from operating system or application operation, and file system data structures. Electronic storage device users typically do not erase or delete this evidence because special software is typically required for that task. However, it is technically possible to delete this information.

c. Files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or cache. The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them.

9. As further described in Attachment B, this application seeks permission to locate not only electronic storage device files that might serve as direct evidence of the crimes described on the warrant, but also for evidence that establishes how electronic storage devices were used, the purpose of their use, who used them, and when.

10. Although some of the records called for by this warrant might be found in the form of user-generated documents (such as word processor, picture, and movie files), electronic storage device storage media can contain other forms of electronic evidence as described below:

a. Data on the storage medium not currently associated with any file can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the electronic storage device was in use. Electronic storage device file systems can record information about the dates files were created and the sequence in which they were created.

b. As explained herein, information stored within an electronic storage device and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within an electronic storage device (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet

history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the electronic storage device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the electronic storage device was remotely accessed, thus inculpating or exculpating the electronic storage device owner. Further, electronic storage device activity can indicate how and when the electronic storage device was accessed or used. For example, as described herein, computers typically contain information that logs computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within an electronic storage device may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer or cellular telephone may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera). The geographic and timeline information described herein may

either inculpate or exculpate the electronic storage device user. Last, information stored within an electronic storage device may provide relevant insight into the device user's state of mind as it relates to the offense under investigation. For example, information within the electronic storage device may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the electronic storage device or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Whether data stored on an electronic storage device is relevant to the investigation may depend on other information stored on the electronic storage device and the application of knowledge about how an electronic storage device works. Therefore, contextual information necessary to understand the evidence described in Attachment B also falls within the scope of the warrant.

d. Further, in finding evidence of how an electronic storage device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, I know from training and experience that it is possible that malicious software can be installed on a

computer, often without the computer user's knowledge, that can allow the computer to be used by others, sometimes without the knowledge of the computer owner.

11. Based upon my knowledge, training and experience, and after having consulted with FBI computer forensic personnel, I know that a thorough search for information stored in storage media often requires agents to seize most or all storage media to be searched later in a controlled environment. This is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. Additionally, to properly examine the storage media in a controlled environment, it is often necessary that some electronic storage device equipment, peripherals, instructions, and software be seized and examined in the controlled environment. This is true because of the following:

a. The nature of evidence. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how an electronic storage device has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable.

b. The volume of evidence. Storage media can store the equivalent of millions of pages of information. Additionally, a suspect may try to conceal criminal evidence; he or she might store it in random order with deceptive file names. This may require searching authorities to peruse all the stored data to determine which particular files are evidence or instrumentalities of crime. This sorting process can take weeks or

months, depending on the volume of data stored, and it would be impractical and invasive to attempt this kind of data search on-site.

c. Technical requirements. Electronic storage devices can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of electronic storage device hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on-site. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

d. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

12. In light of these concerns, I hereby request the Court's permission to seize the electronic storage devices, associated storage media, and associated peripherals that are believed to contain some or all of the evidence described in the warrant, and to conduct an off-site search of the hardware for the evidence described, if, upon arriving at the scene, the agents executing the search conclude that it would be impractical to search the hardware, media, or peripherals on-site for this evidence.

13. I know that when an individual uses a computer to commit crimes involving child pornography, the individuals' computer and/or electronic devices will

generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic storage device is an instrumentality of the crime because it is used as a means of committing the criminal offense. From my training and experience, I believe that an electronic storage device used to commit a crime of this type may contain data that is evidence of how the electronic storage device was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

BIOMETRIC ACCESS TO DEVICES

14. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

15. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing

the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

16. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called "Trusted Face." During the Trusted Face registration process, the user holds the device in front of his or her face. The device's front-facing camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Trusted Face.

17. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-

recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

18. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

19. As discussed in this Affidavit, I have reason to believe that one or more digital devices will be found during the search. The passcode or password that would unlock the devices subject to search under this warrant currently is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the devices, making the use of biometric features necessary to the execution of the search authorized by this warrant.

20. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when: (1) more than 48 hours has elapsed since the device was

last unlocked; or (2) when the device has not been unlocked using a fingerprint for 8 hours and the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

21. Due to the foregoing, if law enforcement personnel encounter any devices that are subject to seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, I request authority for law enforcement personnel to: (1) press or swipe the fingers (including thumbs) of the residents of the SUBJECT PREMISES to the fingerprint scanner of the devices found at the SUBJECT PREMISES; (2) hold the devices found at the SUBJECT PREMISES in front of the residents' face to activate the facial recognition feature; and/or (3) hold the devices found at the SUBJECT PREMISES in front of the residents' face and activate the iris recognition feature, for the purpose of attempting to unlock the devices in order to search the contents as authorized by this warrant.

BACKGROUND ON DISCORD

22. Discord is a messaging platform where millions of users from around the world connect with each other through chat, voice, and video. Discord has both a desktop

(PC, Mac, Linux) application and a mobile (iOS, Android) application, and the service can also be accessed from the website directly at www.discordapp.com.

23. In order to use the services, users need to create an account by selecting a username. Once they've made their account, users can create a server and invite their friends to join it with an invite link, or they can join an existing server. Servers are broken down into sub-categories or "channels" where users can connect with each other by either chatting or calling. Users can also communicate through direct messages, which are private chats created between 1-10 users.

24. To create a Discord account, the user is also required to provide an email address which is verified by Discord.

25. Providers like Discord, Inc. typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account, and other log files that reflect usage of the account. In addition, providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the SUBJECT ACCOUNT.

26. In some cases, Discord users will communicate directly with a provider about issues relating to their account, such as technical problems, billing inquiries, or complaints from other users. Providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications.

BACKGROUND OF THE INVESTIGATION AND PROBABLE CAUSE

27. On or about September 21, 2022, FBI Kansas City received a report of a subject engaged in the production of child sexual abuse material (CSAM). The subject, Eduardo Gonzales, was identified as a family friend who had sexually abused the complainant's 17-year-old daughter (Victim 1) since she was in approximately the sixth grade.

28. On or about September 22, 2022; Victim 1 was interviewed and disclosed that Gonzales would force Victim 1 to dress in different lingerie and then Gonzales would take pictures of Victim 1.

29. On or about September 22, 2022, Gonzales was interviewed, and admitted that he bought Victim 1 lingerie and would then take pictures of her wearing it. Gonzales disclosed that this then progressed to Gonzales taking naked pictures of Victim 1. Gonzales also disclosed that Gonzales operated a Discord account where Gonzales pretended to be Victim 1 in order to "catch" other users who were interested in underage girls.

30. On or about September 22, 2022, Gonzales provided written consent for FBI Kansas City to assume his online identity pertaining to multiple accounts. This included Gonzales' Discord account, "MinxyRose#0054" (hereinafter "MinxyRose"). This is the account that Gonzales used when he pretended to be Victim 1.

31. On or about November 3, 2022, I obtained a search warrant in the Eastern District of Wisconsin for the SUBJECT ACCOUNT and served the search warrant on Discord Inc. On or about November 8, 2022 Discord Inc. provided a response to the search warrant which contained information and content related to the SUBJECT ACCOUNT.

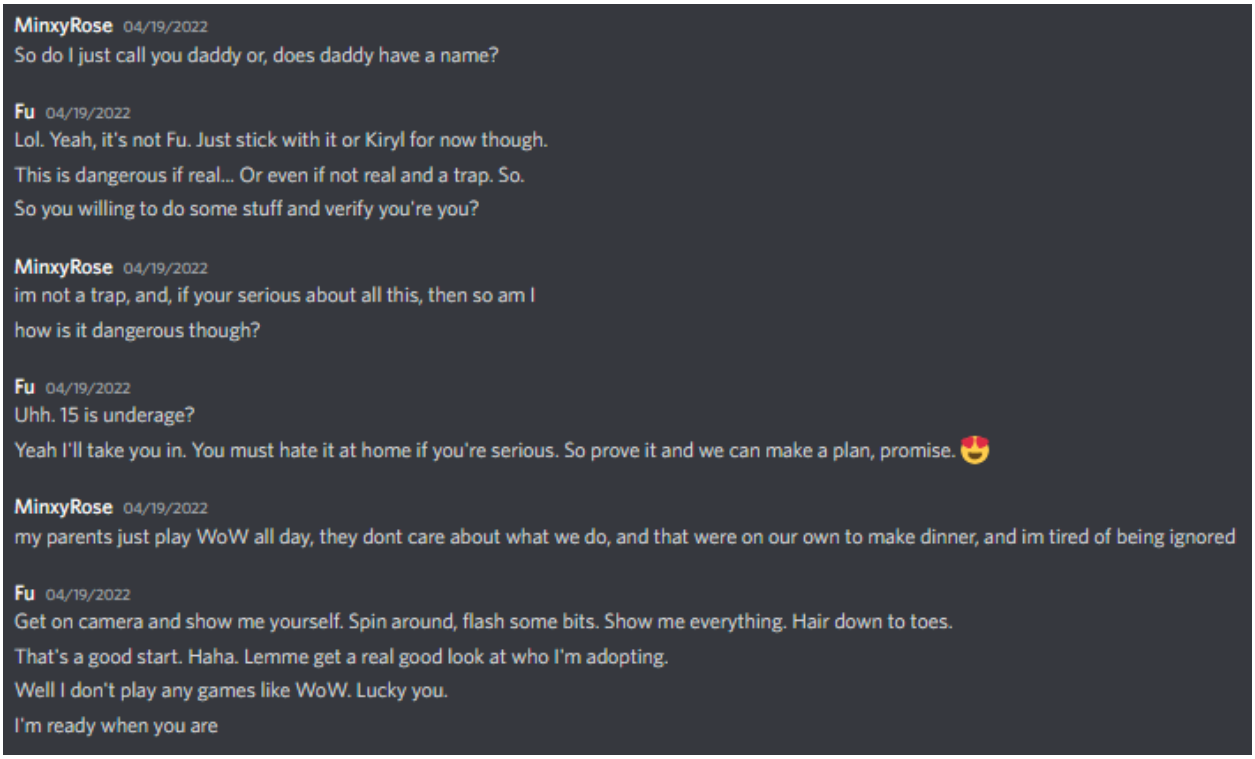
32. On or about October 4, 2022 an FBI Task Force Officer, operating in an online undercover capacity, (hereinafter "FBI-OCE"), logged into the Discord account MinxyRose and directed his investigative focus to Discord user "Fu#9282" (hereinafter the "SUBJECT ACCOUNT") because the SUBJECT ACCOUNT was identified as an account exchanging CSAM and discussing possibly meeting MinxyRose, who the user of the SUBJECT ACCOUNT believed to be 15 years old.

33. The conversation between MinxyRose and the user of the SUBJECT ACCOUNT, that FBI-OCE was able to see once he logged on, started on or about April 19, 2022. At that time, Gonzales was operating the MinxyRose account. It is not known at this time if there were any prior communications between the two accounts.

34. On or about April 19, 2022, the SUBJECT ACCOUNT sent a message to MinxyRose which stated, "much better here than rph." I know from my review of the Discord search warrant material that the SUBJECT ACCOUNT was a member of a group

called "Role Play Haven." This appears to show that the user of the SUBJECT ACCOUNT and MixyRose met in that group, although it is still not known if there were any prior communications. Despite being in a "role play" group, the user of the SUBJECT ACCOUNT, as shown in the next paragraph states "this is dangerous if real," and as described in subsequent paragraphs requests, sends, and possesses images consistent with CSAM.

35. On or about April 19, 2022, the following chat exchange took place between Gonzales as MinxyRose, and the user of the SUBJECT ACCOUNT[1]:

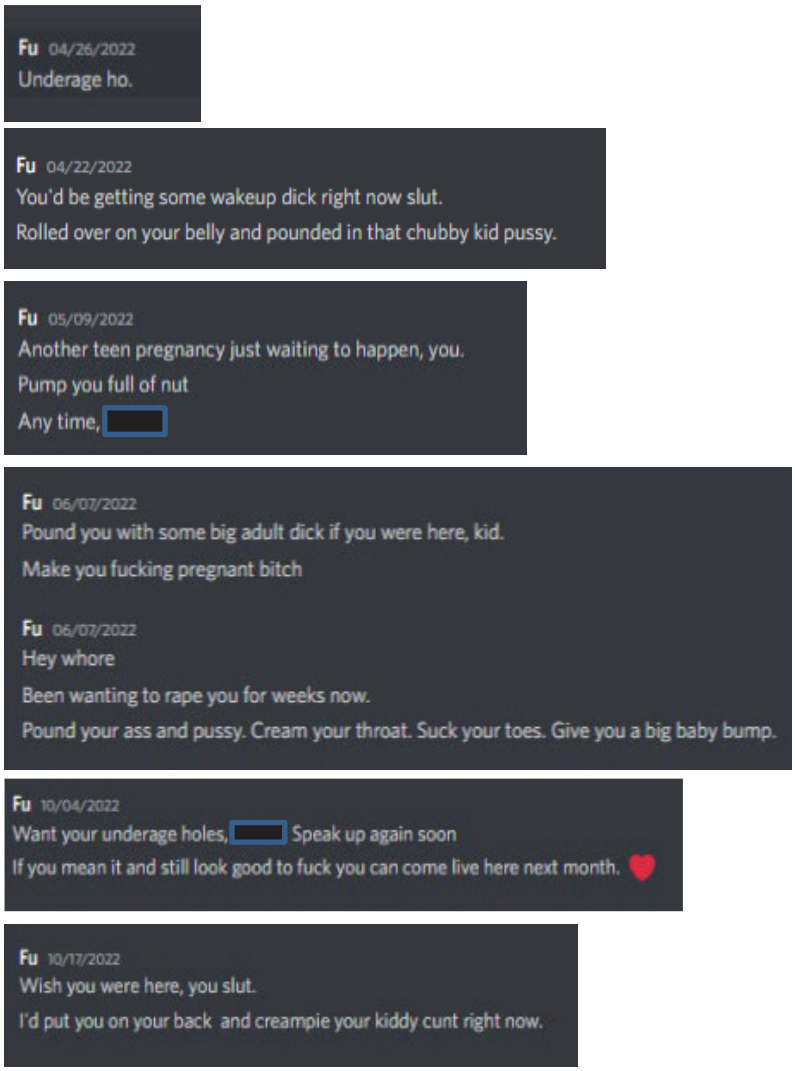


[1] This is a screen capture of the messages between MinxyRose and Fu taken by FBI-OCE subsequent to the account takeover. No times were shown in the screen capture.

36. In these messages, the user of the SUBJECT ACCOUNT is confirming that the user believes MinxyRose to be 15 years old.

37. The user of the SUBJECT ACCOUNT is also requesting that MinxyRose "flash some bits. Show me everything." Subsequent to that message from the user of the SUBJECT ACCOUNT, MinxyRose sent a video which showed Victim 1, from the waist up, nude and exposing Victim 1's breasts to the camera.

38. On multiple occasions the user of the SUBJECT ACCOUNT made reference to MinxyRose being underage, or a kid. These messages show that the user of the SUBJECT ACCOUNT believed that the user was chatting with a minor. These messages and the date they were sent are below[2]:



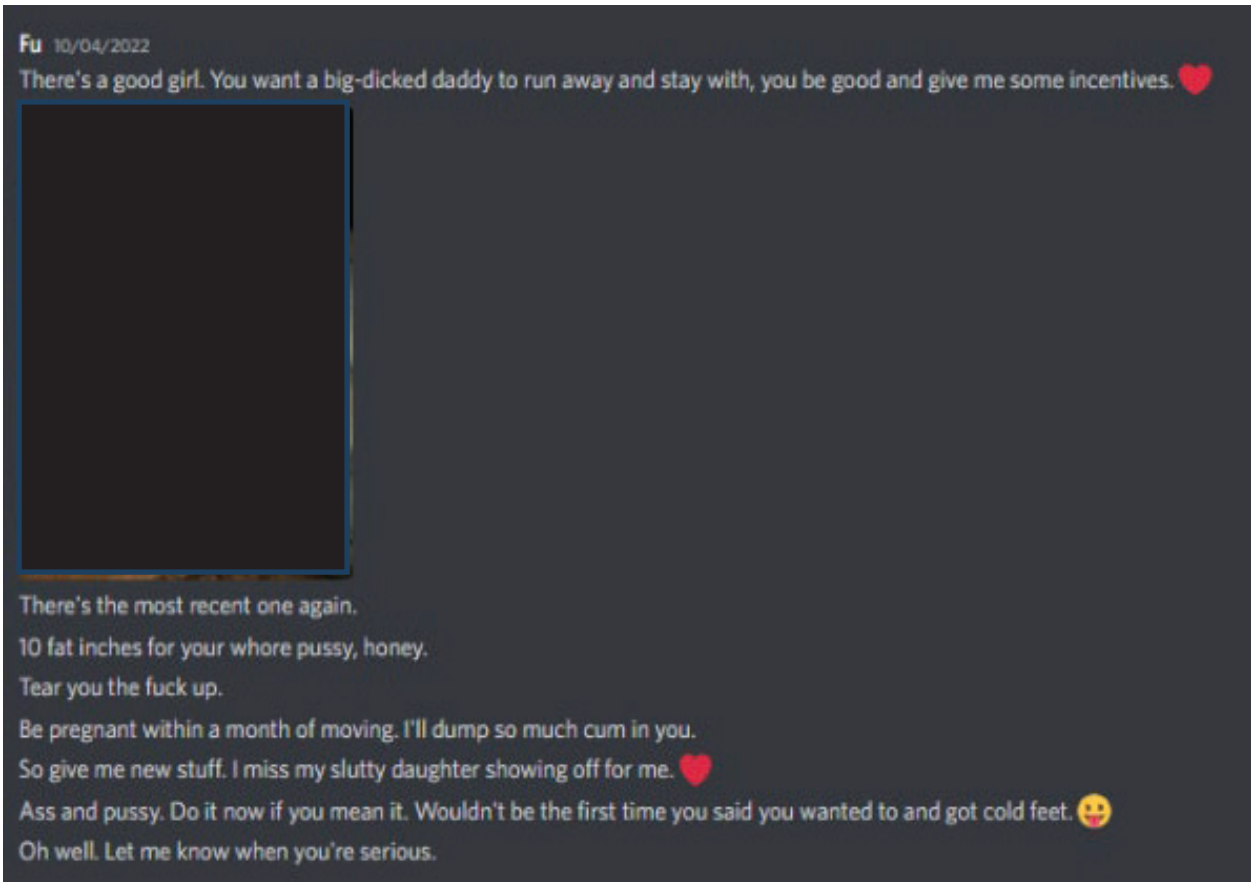
[2] The name of Victim 1 was used in the chats, but it has been redacted from these messages to protect the identity of Victim 1.

39. On or about May 31, 2022, the user of the SUBJECT ACCOUNT sent three images to MinxyRose. The first two images were sexually explicit images of a female kneeling down with her buttocks towards the camera and her nude anus exposed. The third image, consistent with the definition of CSAM, showed Victim 1 lying on her back on a bed, her hair in pigtails, nude except for white stockings, with her legs spread and her nude vagina exposed to the camera. After the first image the user of the SUBJECT ACCOUNT sent a message which stated "Fat whore. Knock you the fuck up." After the third image the user of the SUBJECT ACCOUNT sent a message which stated "Sailor moon[3] looking bitch begging for it. What a whore." During this chat exchange the user of the SUBJECT ACCOUNT sent at least one image consistent with the definition of child pornography.

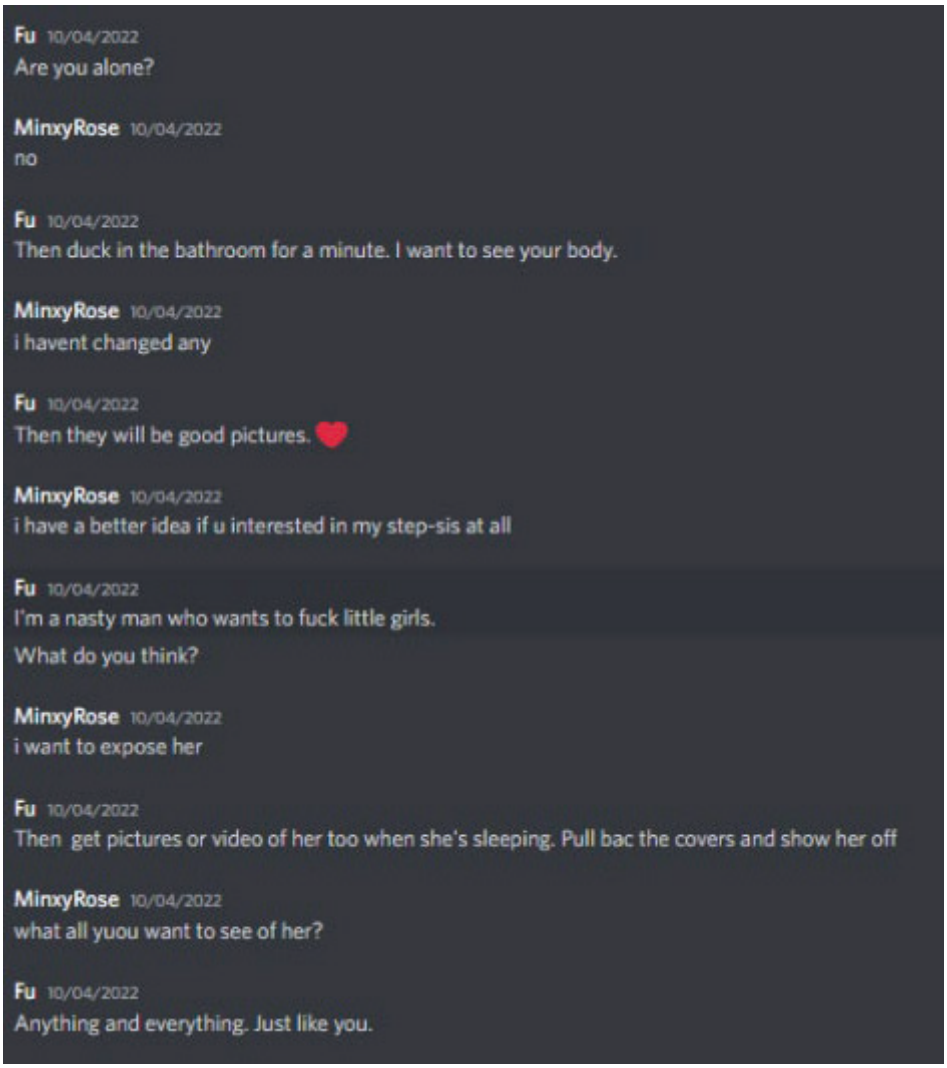
40. On multiple occasions the user of the SUBJECT ACCOUNT requested that MinxyRose send the user nude images. One example of a message where the user of the SUBJECT ACCOUNT requested nude images is below[4]:

[3] Sailor moon is a popular female cartoon character who wore her hair in pigtails.

[4] The redacted portion of this chat is a zoomed in image of an erect male penis.



41. In another instance while FBI-OCE was operating MinxyRose, MinxyRose told the SUBJECT ACCOUNT that MinxyRose had an 8-year-old stepsister. After this, the user of the SUBJECT ACCOUNT told MinxyRose to take pictures of the 8-year-old. The messages are below:



42. These chats show that the user of the SUBJECT ACCOUNT, knew that MinxyRose was a minor, received sexually explicit images and videos from MinxyRose, and requested that MinxyRose self-produce further sexually explicit images and videos of MinxyRose and the 8-year-old stepsister.

IDENTIFICATION OF THE SUBJECT

43. On or about September 30, 2022; a Task Force Officer (TFO) with the FBI sent an administrative subpoena to Discord Inc. regarding the SUBJECT ACCOUNT. On

or about October 3, 2022, Discord Inc. provided a response to the administrative subpoena. The response contained a log of IP addresses used to access the SUBJECT ACCOUNT, as well as the verified email address jbernier2005@hotmail.com.

44. In the Discord Inc. search warrant return I observed a conversation between the SUBJECT ACCOUNT and another account (ACCOUNT 2). There was no CSAM shared between the SUBJECT ACCOUNT and ACCOUNT 2, however, the user of ACCOUNT 2 regularly referred to the user of the SUBJECT ACCOUNT as "James." The user of ACCOUNT 2 was paying the user of the SUBJECT ACCOUNT to write game reviews for the user of ACCOUNT 2.

45. In the Discord Inc. search warrant return I observed an image sent by the user of the SUBJECT ACCOUNT to ACCOUNT 3, on or about June 29, 2022, which showed a white male, shirtless, with his face partially covered with his hand, taking a picture in a mirror. This male had dark facial hair and appeared to be tall and heavyset. After sending the image the user of the SUBJECT ACCOUNT stated "Gotta hide my face too. Never know." The nature of the conversation between the SUBJECT ACCOUNT and ACCOUNT 3 was sexually explicit in nature and the user of ACCOUNT 3 described themselves as almost 14 years old. At this time, it is not known how old the user of ACCOUNT 3 actually was, however the user of the SUBJECT ACCOUNT appeared concerned enough to not show the user's face.

46. In the same conversation the user of the SUBJECT ACCOUNT also described themselves as "Too tall for the door there." In or about June 2022 ACCOUNT

3 asked the user of the SUBJECT ACCOUNT how tall the user of the SUBJECT ACCOUNT was. The user of the SUBJECT ACCOUNT responded "Uh. Very tall. You wouldn't believe it… 6'8". 6'9" with my boots on?" Per the Wisconsin Department of Transportation, BERNIER is 6'8" tall and over 300 pounds. The stature, and facial hair of the male in the image sent to ACCOUNT 3 are consistent with images seen of BERNIER on BERNIER's Facebook, and LinkedIn profiles as well as BERNIER's driver's license photograph.

47. In or about August 2022, the user of the SUBJECT ACCOUNT started a conversation with ACCOUNT 4, which lasted until approximately October 23, 2022. This conversation was sexually explicit in nature, however, the user of ACCOUNT 4 appeared to identify as an adult and the user of the SUBJECT ACCOUNT referred to the user of ACCOUNT 4 as "woman" on multiple occasions.

48. There were at least nine (9) images shared by the user of the SUBJECT ACCOUNT to ACCOUNT 4 which showed clear images of the user's face. Each of the images showed the same white male with dark hair, with varying amounts of dark facial hair. One image was taken in a mirror, shirtless, with the male's face visible. The male's body type matched the shirtless image sent to ACCOUNT 3. The user of the SUBJECT ACCOUNT did not appear to have any reservations about showing his face in this conversation where the user of ACCOUNT 4 did not identify as a child.

49. On or about October 4, 2022 the user of the SUBJECT ACCOUNT told the FBI-OCE, while operating MinxyRose, that it was the user's birthday. BERNIER's birthday is October 4, 1986.

50. On or about December 28th, 2022 BERNIER was evicted from a prior known address in Milwaukee.

51. On or about January 12, 2023 an administrative subpoena was served on Discord, Inc. by an FBI Operational Support Technician regarding the SUBJECT ACCOUNT. On or about January 13, 2023 Discord, Inc. provided a response to the subpoena and showed that the SUBJECT ACOUNT was still active.

52. On or about January 12, 2023 a search warrant was obtained in the Eastern District of Wisconsin for location information related to the known phone number of BERNIER, 414-305-2399.

53. The location information received by the FBI from BERNIER's cell phone carrier, Verizon, placed the device frequently in the general vicinity of the SUBJECT PREMISES.

54. On or about January 23, 2023 FBI Special Agents conducted surveillance in the vicinity of the SUBJECT PREMISES and observed BERNIER approaching the SUBJECT PREMISES at approximately 7:38 AM. BERNIER was seen walking towards the back of the hotel, and likely entered in a side door as he was not observed leaving the vicinity of the hotel.

55. On or about January 24, 2023 a Task Force Officer (TFO) with FBI Milwaukee went to the Biller Hotel to request information related to the occupants of the hotel. The hotel management informed the TFO that BERNIER was staying in Room 105, the SUBJECT PREMISES.

56. Due to the mobile nature and monetary value of technology, there is probable cause to believe that BERNIER brought any electronic devices with him when he moved from his prior residence to the SUBJECT PREMISES and evidence of violations of federal law could be found on the devices.

57. Based upon the above information there is probable cause to believe that BERNIER is the user of the SUBJECT ACCOUNT and is currently residing at the SUBJECT PREMISES.

BACKGROUND ON CHILD PORNOGRAPHY, COMPUTERS, AND THE INTERNET

58. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following:

a. Computers, cellular telephones, and other electronic storage devices (collectively electronic storage devices) have dramatically changed the way in which individuals interested in child pornography interact with each other. Electronic storage devices basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

b. Child pornographers can now transfer printed photographs into a computer-readable format with a device known as a scanner. Furthermore, with the

advent of digital cameras, when the photograph is taken it is saved as a digital file that can be directly transferred to a device by simply connecting the camera to the electronic storage device. In the last ten years, the resolution of pictures taken by digital cameras has increased dramatically, meaning the photos taken with digital cameras have become sharper and crisper. Photos taken on a digital camera are stored on a removable memory card in the camera. These memory cards often store terabytes of data, which provides enough space to store thousands of high-resolution photographs. Video recorders, which once recorded video onto tapes or mini-CDs, now can save video footage in a digital format directly to a hard drive in the camera. The video files can be easily transferred from the video recorder to a computer. Many electronic storage devices (e.g., computers, cellular telephones, and tablets), have cameras built into the device which allows users to create and store still and video images on the device. Moreover, if the device has internet connectivity, users can distribute still and video images from the device.

c. Internet-enabled electronic storage devices can connect to other internet-enabled devices the world over. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography. Child pornography can be transferred via electronic mail or through file transfer protocols (FTPs) to anyone with access to an internet-enabled electronic storage device. Because of the proliferation of commercial services that provide electronic mail

service, chat services (i.e., "Instant Messaging"), and easy access to the Internet, electronic storage devices are the preferred method of distribution and receipt of child pornographic materials.

d. Electronic storage devices are the ideal repository for child pornography. The amount of information that an electronic storage device can hold has grown exponentially over the last decade. Electronic storage devices can store thousands of images at very high resolution. In addition, there are numerous options available for the storage of computer or digital files. One-terabyte external and internal hard drives are not uncommon. Other media storage devices include CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices that are plugged into a port on a computer or other electronic storage device. It is extremely easy for an individual to take a photo with a digital camera, upload that photo to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices (CDs and DVDs are unique in that special software must be used to save or "burn" files onto them). Many electronic storage devices can easily be concealed and carried on an individual's person.

e. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

f. Individuals also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Google,

among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any internet-enabled electronic storage device. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's electronic storage device in most cases.

g. As is the case with most digital technology, communications by way of electronic storage device can be saved or stored on the device. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, an electronic storage device user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

h. Based on my knowledge, training, and experience, I know that electronic files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later

using forensic tools. This is so because when a person "deletes" a file on a device, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

59. Based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact disks, magnetic tapes, memory cards, memory chips, and online or offsite storage servers maintained by corporations, including but not limited to "cloud" storage.

60. Additionally, based upon my training and experience and information related to me by agents and others involved in the forensic examination of computers, I know that routers, modems, and network equipment used to connect computers to the Internet often provide valuable evidence of, and are instrumentalities of, a crime. This is equally true of so-called "wireless routers," which create localized networks that allow individuals to connect to the Internet wirelessly. Though wireless networks may be "secured" (in that they require an individual to enter an alphanumeric key or password before gaining access to the network) or "unsecured" (in that an individual may access the wireless network without a key or password), wireless routers for both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime—including, for example, serving as the instrument through

which the perpetrator of the Internet-based crime connected to the Internet and, potentially, containing logging information regarding the time and date of a perpetrator's network activity as well as identifying information for the specific device(s) the perpetrator used to access the network. Moreover, I know that individuals who have set up either a secured or unsecured wireless network in their residence are often among the primary users of that wireless network.

61. Based on my previous investigative experience related to child exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who transport, distribute, receive, possess, and/or access with intent to view child pornography:

a. Such individuals may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

b. Such individuals may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner,

or to demonstrate the desired sexual acts.

c. Likewise, such individuals often maintain their child pornography images in a digital or electronic format in a safe, secure, and private environment, such as a computer and surrounding area. These child pornography images are often maintained for several years and are kept close by, usually at the possessor's residence, inside the possessor's vehicle, or, at times, on their person, to enable the individual to view the child pornography images, which are valued highly. Some of these individuals also have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis.

d. Importantly, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices using forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual "deleted" it.

e. Such individuals also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

f. Such individuals prefer not to be without their child pornography

for any prolonged period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world. Thus, even if an individual, uses a portable device (such as a mobile phone) to access the internet and child pornography, it is more likely than not that evidence of this access will be found in the SUBJECT PREMISES, or a device located on BERNIER, as set forth in Attachment A.

46. BERNIER, who was sharing child pornography at the SUBJECT PREMISES likely displays characteristics common to individuals who possess, access with intent to view, and distribute child pornography based on his history of distributing child exploitation material as set forth in this affidavit.

CONCLUSION

47. I respectfully request that this Court issue a search warrant for the location, and search of person described in Attachment A authorizing the seizure and search of the items described in Attachment B.

ATTACHMENT A
DESCRIPTION OF LOCATIONS TO BE SEARCHED

(1) The Biller Hotel property located at 725 N 22nd St, Milwaukee, WI 53233 (photo below) limited to Room 105. The Biller Hotel is a four story, brick façade building with a green awning over the front entrance. The hotel is divided into multiple different individual rooms. The search will be limited to the room labeled 105.

(2) the person of James Bernier, DOB 10/4/1986.

ATTACHMENT B

LIST OF ITEMS TO BE SEIZED

1. Cell phones, computer(s), computer hardware, computer software, computer related documentation, computer passwords and data security devices, videotapes, video recording devices, video recording players, and video display monitors that may be, or are used to: visually depict child pornography or child erotica; display or access information pertaining to a sexual interest in child pornography; display or access information pertaining to sexual activity with children; or distribute, possess, or receive child pornography, child erotica, or information pertaining to an interest in child pornography or child erotica.
2. Any and all computer software, including programs to run operating systems, applications (such as word processing, graphics, or spreadsheet programs), utilities, compilers, interpreters, and communications programs.
3. Any and all notes, documents, records, or correspondence, in any format and medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and handwritten notes) pertaining to the possession, receipt, or distribution of child pornography as defined in 18 U.S.C. § 2256(8) or to the possession, receipt, or distribution of visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2).
4. In any format and medium, all originals, computer files, copies, and negatives of child pornography as defined in 18 U.S.C. § 2256(8), visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2), or child erotica.

5. Any and all diaries, address books, names, and lists of names and addresses of individuals who may have been contacted by the operator of any device by use of the computer or by other means for the purpose of distributing or receiving child pornography as defined in 18 U.S.C. § 2256(8) or visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2).
6. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and handwritten notes), identifying persons transmitting, through interstate or foreign commerce by any means, including, but not limited to, by the United States Mail or by computer, any child pornography as defined in 18 U.S.C. § 2256(8) or any visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).
7. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, other digital data files and web cache information) concerning the receipt, transmission, or possession of child pornography as defined in 18 U.S.C. § 2256(8) or visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).
8. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) concerning communications between individuals about child pornography or the existence of sites on the Internet

that contain child pornography or that cater to those with an interest in child pornography.

9. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) concerning membership in online groups, clubs, or services that provide or make accessible child pornography to members.

10. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) that concern any accounts with an Internet Service Provider.

11. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) that concern online storage or other remote computer storage, including, but not limited to, software used to access such online storage or remote computer storage, user logs or archived data that show connection to such online storage or remote computer storage, and user logins and passwords for such online storage or remote computer storage.

12. Any and all cameras, film, videotapes or other photographic equipment.

13. Any and all visual depictions of minors.

14. Any and all address books, mailing lists, supplier lists, mailing address labels, and any and all documents and records, in any format or medium (including, but not

limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files), pertaining to the preparation, purchase, and acquisition of names or lists of names to be used in connection with the purchase, sale, trade, or transmission, through interstate or foreign commerce by any means, including by the United States Mail or by computer, any child pornography as defined in 18 U.S.C. § 2256(8) or any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

15. Any and all diaries, notebooks, notes, and any other records reflecting personal contact and any other activities with minors visually depicted while engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

16. For any electronic storage device, computer hard drive, electronic device, or other physical object upon which electronic information can be recorded (hereinafter, "electronic storage device") that is called for by this warrant, or that might contain things otherwise called for by this warrant:

    a. evidence of who used, owned, or controlled the electronic storage device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

    b. evidence of software that would allow others to control the electronic storage device, such as viruses, Trojan horses, and other forms of malicious software, as

well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence indicating how and when the electronic storage device was accessed or used to determine the chronological context of electronic storage device access, use, and events relating to crime under investigation;

e. evidence indicating the electronic storage device user's location and state of mind as it relates to the crime under investigation;

f. evidence of the attachment to the electronic storage device of other storage devices or similar containers for electronic evidence;

g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the electronic storage device;

h. evidence of the times the electronic storage device was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the electronic storage device;

j. documentation and manuals that may be necessary to access the electronic storage device or to conduct a forensic examination of the electronic storage device;

k. contextual information necessary to understand the evidence described in this attachment.

17. Records and things evidencing the use of the Internet Protocol addresses to communicate with the internet, including:

a. routers, modems, and network equipment used to connect electronic storage devices to the Internet;

b. records of Internet Protocol addresses used;

c. records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

As used above, the terms "records" and "information" include all the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of electronic storage device or electronic storage; any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form.

During the execution of the search of the premises described in Attachment A, law enforcement personnel are authorized to press the fingers (including thumbs) of individuals found at the premises to the Touch ID sensor of device(s) or scan for facial recognition, such as an iPhone. Android, or Tablet, found at the premises for the purpose of attempting to unlock the device via fingerprint or facial recognition in order to search the contents as authorized by this warrant. If facial recognition is required, the subject(s) will remain still and look, with eyes open, at the camera for any devices seized in connection if this warrant for the purpose of attempting to unlock the device(s) in order to search the contents as authorized by this warrant.